01net
OK
nos newsletters
nos magazines
01net Lisez 01net pour 2,45 € / n° seulement

Les publicitaires vous espionnent et vous n'y pouvez plus rien !

Des chercheurs américains et belges ont démontré une nouvelle technique permettant d'identifier un navigateur ou une machine afin de suivre en permanence son comportement de surf, sans moyen de la bloquer.

Pierre Fontaine | 01net. | le 22/07/14 à 19h01 | laisser un avis

Tweet

Les cookies vous les connaissez, depuis le temps que vous les côtoyez, et vous vous en méfiez comme de la peste, eux qui disent tout de votre navigation sur le Web. Avec l'aide de quelques logiciels adéquats, vous avez même réussi à les faire taire et à surfer en vous disant que la Toile était encore un espace de liberté non surveillée. Ca, c'était jusqu'au 1er juillet dernier.

Surfez, vous êtes identifié

Enfin, disons que c'est la date à laquelle l'illusion a pris un sérieux coup dans l'aile. C'est en effet le 1er juillet dernier que des chercheurs de l'université de Louvain et de Princeton ont publié un rapport sur une de leur découverte : une application d'une méthode de pistage de l'utilisateur en ligne, théorisée pour la première fois en 2012.
Cette technique s'appelle *canvas fingerprinting* et consiste à demander au navigateur de générer une image cachée à partir de texte.
Selon ces chercheurs, en utilisant l'API Canvas, implémentée dans les navigateurs récents, il est possible d'identifier de manière unique – d'où le terme d'empreinte – un navigateur ou un appareil qui accède au Web. La différence permettant l'identification se ferait dans la façon dont est « rendu » le texte.
Ce dernier sera affiché différemment en fonction du système d'exploitation, de la librairie de polices de caractère, de la carte graphique et de ses pilotes, du navigateur, des réglages de l'anti-aliasing, du « lissage des sous-pixels » et même l'écran.
Il suffirait d'une fraction de seconde pour que cette empreinte soit prise, sans bien sûr que l'utilisateur soit au courant et sans qu'il ne puisse vraiment s'y opposer.

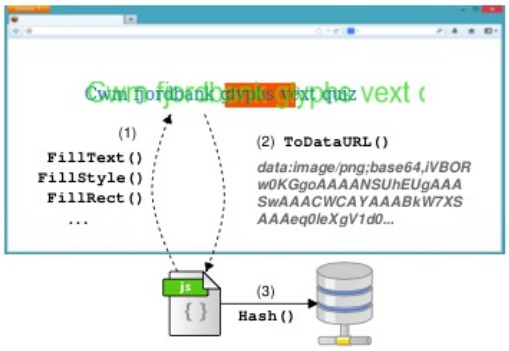

Figure 1: Canvas fingerprinting basic flow of operations

Schéma explicatif du fonctionnement de base du canvas fingerprinting.

Une tendance encore naissante

Pour prendre la mesure de la menace qui pèse sur nos épaules, les six chercheurs sont partis à la chasse au script permettant au « canvas » d'identifier un appareil. Le résultat est assez

@01net sur twitter

à lire aussi
SUR LES MÊMES THÈMES

- La Shield Tablet de Nvidia en avant première (vidéo)
- Maison connectée : à quoi sert un lave-linge communicant ? (vidéo du jour)
- Le robot Jibo, l'ami de la famille qui rêve de trôner dans votre salon
- Qleek : la start-up qui veut rematérialiser vos musiques, films, et photos (vidéo)
- Maison connectée : ces robots de nettoyage sont décevants (vidéo du jour)
- Maison connectée : semaine spéciale sur 01netTV (vidéo)
- Tout sur l'ultra HD : 01netTV vous répond (vidéo)
- JTech 194 : LG G Watch, Top 5 des smartphones haut de gamme, OnePlus One (vidéo)
- La voiture du futur selon Carlos Ghosn
- Que cache la restructuration massive de Microsoft ? (vidéo du jour, #01Live)
- Les voitures autonomes sont des «armes mortelles» aux yeux du FBI
- 01LIVE HEBDO #24 : le debrief de l'actu High-tech (vidéo replay)
- Roaming: Free ajoute les SMS illimités en Europe à son forfait 19,99 euros
- Le Top 5 des smartphones haut de gamme (vidéo du jour)
- Tesla Model 3, la nouvelle berline-compacte électrique américaine
- Phone Apps #61 : top 10 des meilleures applis photo pour iPhone (vidéo)
- La G Watch de LG tient-elle ses promesses ? (vidéo du jour)
- Novartis et Google s'allient pour développer les lentilles intelligentes
- OnePlus One : le smartphone le plus puissant du marché (vidéo du jour)

impressionnant. Sur les 100 000 sites les plus fréquentés dans le monde selon Alexa, plus de 5,5% de ces sites contiennent le script.
Nos confrères de *Propublica* indiquent que des sites aussi différents que YouPorn.com ou WhiteHouse.org sont ainsi concernés par ce système de « suivi ». Mais le plus intéressant est de constater que 95% de ces espions proviennent d'une seule et même source : Addthis. Une société, fondée en 2006, qui *« combine les meilleurs outils marketing du Web avec le big data et les services de ciblage de l'audience »*.

Difficile, voire impossible à bloquer

Le problème de cette méthode d'identification est qu'elle ne peut pas être bloquée en utilisant les outils habituels garantissant notre vie privée en ligne, qu'ils soient intégrés aux navigateurs ou installés par l'utilisateur, comme AdBlock Plus.
Mais cette relative impossibilité à bloquer cette prise d'empreinte de la machine est d'autant plus inquiétante qu'elle semble pouvoir être mise en place à l'insu de l'administrateur du site. Ainsi, *Propublica* indique que YouPorn a annoncé ne pas être au courant de la présence de ce « module » sur son site. Il est en effet présent dans l'outil de partage social d'AddThis.
Evidemment, comme pour les cookies, qu'ils soient permanents ou temporaires, l'objectif de ce *canvas fingerprinting* est de récolter des données sur les utilisateurs pour pouvoir dresser leur profil. Richard Harris, directeur général d'AddThis, ne s'en cache d'ailleurs pas. Il déclarait à nos confrères : *« Nous cherchons une alternative aux cookies »*. C'est pourquoi sa société a commencé à les tester en début d'année. Evidemment ses équipes se sont posées la question du respect de la vie privée avant de se lancer dans cette opération mais ont conclu que ce procédé *« s'inscrivait parfaitement dans les règles et régulations, lois et règlements que nous avons »*.
Les Internautes sont évidemment tout à fait en droit de ne pas être de cet avis, même si effectivement l'empreinte n'est qu'un chiffre et n'est pas associé à un nom ou à une personne… Pour autant, la vie privée semble bien mal en point.

La bonne nouvelle pourrait être que cette technologie ne semble être précise qu'à 90% et ne pas bien fonctionner sur mobile. Or, c'est sur cette plate-forme que se porte actuellement le marché publicitaire. Le *canvas fingerprinting* pourrait donc ne pas devenir le remplaçant tant attendu des cookies. Un vague espoir alors que le débat sur le *Do Not Track* continue de s'enliser et semble tout à coup bien obsolète.

A lire aussi :
Yahoo! abandonne le Do Not Track – 02/05/2014

Sources :
Etude universitaire des universités de Louvain et Princeton (PDF) via ProPublica

envoyer par mail imprimer l'article Tweet
Suivre @01net

Actu précédente
La Shield Tablet de Nvidia en avant première (vidéo)

01net
CGV - Conditions d'abonnement - Charte de confiance - Recrutement - Contacts - Mentions légales et CGU
NextInteractiveMedia : 01net - RMC - RMC SPORT - RMC DÉCOUVERTE - BFMTV - BFM BUSINESS - 01Business - Association RMC/BFM
lecharger.com OK GUIDE D'ACHAT ASTUCES